Best Practices Guide for Anti-Spoofing

Contents

About this document
What is Email Spoofing?
Email Spoofing Defence Workflow
Layer 1: Validity Check on the Sender’s Domain
Layer 2: Verify the “From” header using DMARC
Layer 3: Prevent Spammers from Sending Spoofed Emails
Layer 4: Determine Malicious Senders via Email Domain
Layer 5: Reduce False Positives with SPF or DKIM Verification Results
Layer 6: Detect Messages with Possibly Forged Sender Name
Layer 7: Positively Identified Spoofing Email
Layer 8: Protecting Against Phishing URLs
Layer 9: Augment Spoofing Detection Capability with Cisco Advanced Phishing Protection (APP)
What More You Can Do with Spoofing Prevention?

About this document

This document is for Cisco Customers, Cisco Channel Partners and Cisco Engineers who will deploy Cisco Email Security. This document covers:

- What is Email Spoofing?
- Email Spoofing Defence Workflow
- What more you can do with spoofing prevention?

What is Email Spoofing?

Email Spoofing is email header forgery where the message appears to have originated from someone or somewhere other than the actual source. Email Spoofing is a tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate, trustworthy source. For more information about spoofing, please refer to [http://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it](http://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it)

Email Spoofing falls into the following categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Domain</td>
<td>Impersonate an identical domain in the “Envelope From” as the recipient’s domain.</td>
</tr>
<tr>
<td>Spoofing</td>
<td>The “From” header shows a legitimate sender with a name of an organization. Known as Business Email Compromise (BEC).</td>
</tr>
<tr>
<td>Display Name</td>
<td>The “From” header shows a legitimate sender with the brand name of an organization.</td>
</tr>
<tr>
<td>Deception</td>
<td>An email with an URL that attempts to steal sensitive data and / or login information from the victim. A fake email from a bank asking you to click a link and verify your account details is an example of phishing URL based</td>
</tr>
<tr>
<td>Brand Name</td>
<td></td>
</tr>
<tr>
<td>Impersonation</td>
<td></td>
</tr>
<tr>
<td>Phish URL Based</td>
<td></td>
</tr>
<tr>
<td>Attack</td>
<td></td>
</tr>
</tbody>
</table>

Main Target:
- Employees
- Customers
- Partners
Cousin or Look-alike Domain Attack

The “envelope from” or “From” header value shows a similar sender address that impersonates a real one, in an attempt to bypass SPF, DKIM and DMARC inspections.

Account Takeover / Compromised Account

Gain unauthorized access to a real email account that belongs to someone and then sends emails to other victims as the legitimate email account owner.

The first category relates to abuses of the owner’s domain name in the “Envelope From” value in the internet header of an email. Cisco Email Security can remediate this attack by using sender DNS verification to permit only legitimate senders and the same result can be achieved globally by using DMARC, DKIM and SPF verification.

However, the other categories are not entirely violating the domain portion of the sender’s email address, hence it is not easy to be deterred by using DNS text records or sender verification only. Ideally, it would be best to combine some Cisco Email Security features along with out-the-box based Cisco Advanced Phishing Protection (APP) to fight against such advanced threats. Please note that the application of Cisco Email Security features may vary from one organization to another and improper application can lead to a high incidence of false positives, hence it is important to understand the organization’s business needs and tailor the features accordingly.

Email Spoofing Defence Workflow

The security features that address the best practices for monitoring, warn and enforce against spoofing attacks are shown in the diagram below (Figure 1). The details of each feature will be provided in this document. The best practice is an in-depth defense approach to detect email spoofing. Always keep in mind that attackers will change their methods against an organization over time, so it is very important for an administrator to monitor any occurring changes and follow up with appropriate warnings and enforcement.

Figure 1. Cisco Email Security Spoof Defence Pipeline
Layer 1: Validity Check on the Sender’s Domain

Sender Verification is a simpler way to prevent email sent from a bogus email domain, such as cousin domain spoofing (for example 'c1sc0.com' is the imposter of 'cisco.com'). Cisco Email Security makes an MX record query for the domain of the sender’s email address and performs an A record lookup on the MX record during the SMTP conversation. If the DNS query returns NXDOMAIN, it will treat the domain as non-existence. It is a common technique for attackers to forge the envelope sender information so the email from an unverified sender is being accepted and processed further. Using this feature, all incoming messages that fail the verification check will be rejected by Cisco Email Security unless the sender’s domain or IP address is pre-added in the “Exception Table”.

Best Practice: Configure Cisco Email Security to reject the SMTP conversation if the email domain of the envelope sender field is invalid and only allow legitimate senders by configuring the mail flow policy, sender verification and exception table (optional). For more information, please visit: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/200057-Spoof-Protection-using-Sender-Verification.html

Figure 2. Sender Verification Section in Default Mail Flow Policy.

Layer 2: Verify the “From” header using DMARC

DMARC verification is a much powerful feature to fight against “Direct Domain Spoofing” and also includes “Display Name” & “Brand Impersonation” attacks. DMARC ties in information authenticated with SPF or DKIM (sending domain source, or signature) with what is presented to the end-recipient in the “From” header and ascertains that SPF and/or DKIM identifiers are aligned with the FROM header identifier.

To pass DMARC verification, an incoming email must pass at least one of these authentication mechanisms. Cisco Email Security also allows the administrator to define a DMARC verification profile to override the domain owner’s DMARC policies and send aggregate (RUA) and failure/forensic (RUF) reports to the domain owners which helps to strengthen their authentication deployments in return.

Best Practice: Edit the default DMARC profile that complies with the DMARC policy actions that are advised by the sender. Additionally, the global settings of DMARC verification must be edited to enable correct report generation. Once the profile is configured appropriately, the DMARC
verification service must be enabled in the default policy of the Mail Flow Policies.

**Figure 3. DMARC Verification Profile**

<table>
<thead>
<tr>
<th>Profile Name: DEFAULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Action when the Policy in DMARC Record is Reject:</td>
</tr>
<tr>
<td>No Action</td>
</tr>
<tr>
<td>Quarantine to: Policy</td>
</tr>
<tr>
<td>Reject:</td>
</tr>
<tr>
<td>SMTP Code: 550</td>
</tr>
<tr>
<td>SMTP Response: #5.7.1 DMARC unauthenticated mail</td>
</tr>
<tr>
<td>Message Action when the Policy in DMARC Record is Quarantine:</td>
</tr>
<tr>
<td>No Action</td>
</tr>
<tr>
<td>Quarantine to: Policy</td>
</tr>
<tr>
<td>Accept</td>
</tr>
<tr>
<td>Reject</td>
</tr>
<tr>
<td>SMTP Code: 451</td>
</tr>
<tr>
<td>SMTP Response: #4.7.1 Unable to perform DMARC verification</td>
</tr>
<tr>
<td>Message Action for Temporary Failure:</td>
</tr>
<tr>
<td>No Action</td>
</tr>
<tr>
<td>Quarantine to: Policy</td>
</tr>
<tr>
<td>Accept</td>
</tr>
<tr>
<td>Reject</td>
</tr>
<tr>
<td>SMTP Code: 550</td>
</tr>
<tr>
<td>SMTP Response: #5.7.1 DMARC verification failed.</td>
</tr>
<tr>
<td>Message Action for Permanent Failure:</td>
</tr>
<tr>
<td>No Action</td>
</tr>
<tr>
<td>Reject</td>
</tr>
<tr>
<td>SMTP Code: 550</td>
</tr>
<tr>
<td>SMTP Response: #5.7.1 DMARC verification failed.</td>
</tr>
</tbody>
</table>

**Note:** DMARC must be implemented by the sending domain’s owner in conjunction with a domain monitoring tool, such as Cisco Domain Protection. When implemented appropriately, DMARC enforcement in Cisco Email Security helps protect against phishing email sent to the employees from unauthorized senders or domains. For more information about Cisco Domain Protection, please visit this link: [https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740937.pdf](https://www.cisco.com/c/dam/en/us/products/collateral/security/cloud-email-security/at-a-glance-c45-740937.pdf)

**Layer 3: Prevent Spammers from Sending Spoofed Emails**

Spoofing attacks can be another common form of a spam campaign, hence enabling anti-spam protection is still essential to effectively identify fraudulent emails that contain spam/phishing elements and block it positively. The use of the antispam engine, when coupled with other best practice actions, thoroughly described in this document, provide the best results without the loss of legitimate emails.

**Best Practice:** Enable anti-spam scanning in the default mail policy and set quarantine action to positively identified spam settings. Increase the minimum scanning size for spam message to at least 2M in the global setting.

**Figure 4. Anti-Spam setting in default mail policy**
The Spam Threshold can be adjusted for Positive and Suspected Spam to increase or decrease the sensitivity (Figure 5); however, Cisco discourages the administrator to do so, and only use the default thresholds as a baseline, unless being told otherwise by Cisco.

**Figure 5. Anti-Spam Thresholds setting in default mail policy**

As a side note, Cisco Email Security offers add-on Intelligent Multi-Scan (IMS) engine that provides different combination from the anti-spam engine in favor of increasing the spam catch rates (most aggressive catch-rate).

**Layer 4: Determine Malicious Senders via Email Domain**

Using IP based reputation detection (SBRS) to fight against spoof attacks is no longer sufficient due to several reasons particularly with the fact that the same source of IP addresses can be used to host multiple sending domains, in which case, the nature of each domain may be different, hence making SBRS less effective to prevent the malicious infected messages and spoofing campaigns. Sender Domain Reputation (SDR) comes in handy to address such concerns.

With the preservation of IP reputation filtering at the SMTP connection layer, the reputation verdict based on the sending domain information presented in the SMTP conversation and message headers will be taken into consideration to determine if the email should be permitted by the incoming mail policy or not. SDR is at the top in terms of effectively preventing spoofing campaigns from malicious sources or a domain that has recently been registered, less than a
week, for example, in a clear attempt to outsmart the reputation scanning feature.

**Best Practice:** Create an incoming content filter that captures the sending domain in which SDR reputation verdict falls under either Awful / Poor / Tainted or the Domain Age is less than or equals to 5 days. The recommended action is to quarantine the message and send a notification to the email security administrator and the original recipient. For more information about how to configure SDR, please view the Cisco video at https://www.youtube.com/watch?v=IBLRQMT3SHU

*Figure 6. Content Filter for SDR reputation and domain age with both notify and quarantine actions.*

**Layer 5: Reduce False Positives with SPF or DKIM Verification Results**

It is imperative to enforce SPF or DKIM verification (both or either one) as to build multi-layers of spoof email detection for most attack types. In lieu of taking a final action (such as drop or quarantine), Cisco recommends adding a new header such as [X-SPF-DKIM] on the message that fails SPF or DKIM verification and co-operate the outcome with Forged Email Detection (FED) feature which we will cover later, in favor of an improved catch rate of spoofing emails.

**Best Practice:** Create a content filter that inspects SPF or DKIM verification results of each incoming message that passed through previous inspections. Add a new X-header (for example X-SPF-DKIM=Fail) on the message that fails the SPF or DKIM verification and delivers to the next layer of scanning – Forged Email Detection (FED).

*Figure 7. Content filter that inspects messages with failed SPF or DKIM results*

**Layer 6: Detect Messages with Possibly Forged Sender Name**

Complementing with SPF, DKIM and DMARC verifications, Forged Email Detection (FED) is
another important line of defense against email spoofing. FED is ideal to remediate spoof attacks that abuse the “From” value in the message body. Given that you already know the executive names within the organization, you can create a dictionary of these names and then reference that dictionary with the FED condition in content filters. Apart from executive names, you can also create a dictionary of cousin domains or look-alike domains, based on your own domain by using DNSTWIST (https://github.com/elceef/dnstwist) to match against look-alike domain spoofing.

**Best Practice:** Identify the users in your organization whose messages are likely to be forged. Create a custom dictionary that accounts for executives. For every executive name, the dictionary needs to include the username and all possible usernames as terms (Figure 8). When the dictionary is complete, use Forged Email Detection (FED) in the content filter to match on the “From” value from incoming messages with this dictionary entries.

*Figure 8. Custom Directory for Forged Email Detection*

It is an optional action to add an exception condition for your email domain in the “Envelope Sender” to bypass the FED inspection. Alternatively, a custom “Address List” can be created to bypass the FED inspection to a list of email addresses that are displayed in the “From” header (Figure 9).

*Figure 9. Create Address List to bypass FED inspection*
Apply the Forged Email Detection (FED) proprietary action to strip the “From” value and review the actual envelope sender email address in the message inbox. Rather than applying a final action, add a new X-header (example: X-FED=Match) on the message that matched the condition and continue delivering the message to the next layer of inspection (Figure 10).

Figure 10. Recommended Content Filter Setting for FED

Layer 7: Positively Identified Spoofing Email

It is more effective to identify a real spoofing campaign by referencing other verdicts from various security features in the pipeline, such as the X-header information that is produced by “SPF/ DKIM Enforcement” and “FED”. Administrators can create a content filter to identify messages added with both new X-headers due to failed SPF / DKIM verification results (X-SPF-DKIM=Fail) and which “From” header is matching the FED dictionary entries (X-FED=Match).

The recommended action can be, either quarantine the message and notify the recipient or continue delivering the original message but prepending [POSSIBLE FORGED] words to “Subject” line as a warning to the recipient as depicted below (Figure 11).

Figure 11. Combine all X-headers into a single (final) rule
Layer 8: Protecting Against Phishing URLs

Protection against phishing URL links are incorporated into the URL and Outbreak Filtering in the Cisco Email Security. Blended threats combine spoofing and phishing messages in an attempt to look more legitimate to the target, hence enabling Outbreak Filtering is critical to help detect, analyze and stop such threats on a real-time basis. It is worth knowing that URL reputation is assessed inside of the Anti-Spam engine and will be used as part of the decision for spam detection. If the Anti-Spam engine does not stop the message with URL as Spam, it will be evaluated by both URL and Outbreak Filtering in the latter part of the security pipeline.

Recommendation: Create a content filter rule that blocks URL with a “malicious” reputation score and redirects the URL with a “neutral” reputation score to Cisco Security Proxy (Figure 12). Enable Threat Outbreak Filters by enabling Message Modification. URL Rewrite allows for suspicious URLs to be analyzed by Cisco Security Proxy (Figure 13). For more information, please visit: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118775-technote-esa-00.html

Figure 12. Content Filter for URL Reputations

Figure 13. Enable URL rewrite in Outbreak Filtering
Cisco offers Advanced Phishing Protection (APP) which integrates machine learning, combining local identity and relationship modeling with behavior analytics, to better protect against identity deception-based threats. APP also allows the administrator to remove malicious emails from users' inboxes to prevent wire fraud or other advanced attacks; and provides detailed visibility into email attack activity, including total messages secured and attacks prevented. For more details, please visit the following links:

**Recommendation:** Cisco APP is an out-of-the-box solution in the cloud. Administrators perform email journaling on the email server such as Exchange and Office 365 in order to retain the header information of all incoming messages in Cisco APP for further analysis without any human programming intervention. Administrators review the attack classes that Cisco APP has identified (Figure 14) and configure policies that include the ability to alert the administrator, delete the message or quarantine the message to an alternate folder based on the attack types (Figure 15).

*Figure 14. Cisco APP automatically populate the attack classes on the main dashboard*
What More You Can Do with Spoofing Prevention?

Many spoofs can be remediated by exercising a few simple precautions, including but not limited to:

- Limit the use of whitelisted domains in the Host Access Table (HAT) to a very few core business partners
- Always track and update members in the SPOOF_ALLOW sender group, if you have created one by following the instructions given in the best practices link.
- Enable graymail detection and place them in the spam quarantine as well

But most important of all, enable SPF, DKIM, and DMARC and implement them appropriately. However, the guidance of how to publish SPF, DKIM and DMARC records is beyond the scope of this document. For that, please refer to the following white paper:


We also understand the challenge of remediating email attacks such as the spoofing campaigns discussed here. If you are having questions about implementing these best practices, please contact Cisco Technical Support by opening a case. Alternatively, please reach out to your Cisco Account Team for a solution and design guidance. For more information about Cisco Email Security, please go to http://www.cisco.com/c/en/us/products/security/emailsecurity/index.html